ElectroMagnetic Analysis and Fault Injection onto Secure Circuits

Paolo Maistri, Régis Leveugle, Lilian Bossuet, Alain Aubert, Viktor Fischer, Bruno Robisson, Nicolas Moro, Philippe Maurine, Jean-Max Dutertre, Mathieu Lisart

22nd IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC'14)
doi: 10.1109/VLSI-SoC.2014.7004182

ElectroMagnetic Analysis and Fault Injection onto Secure Circuits

P. Maistri[1], R. Leveugle[1], L. Bossuet[2], A. Aubert[2], V. Fischer[2],
B. Robisson[3], N. Moro[3], P. Maurine[3,4], J.-M. Dutertre[5], M. Lisart[6]

[1] Univ. Grenoble Alpes, TIMA, F-38000 Grenoble
CNRS, TIMA, F-38000 Grenoble
{paolo.maistri, regis.leveugle}@imag.fr

[2] Laboratoire Hubert Curien (CNRS, University of Lyon), 42000 Saint-Etienne, France
lilian.bossuet@univ-st-etienne.fr

[3] CEA-TECH, 880 route de Mimet, 13541 Gardanne, France
{bruno.robisson,nicolas.moro,philippe.maurine}@cea.fr

[4] LIRMM (CNRS, Univ. Montpellier II), 161 Rue Ada, 34292 Montpellier, France
philippe.maurine@lirmm.fr

[5] Ecole Nationale Supérieure des Mines de Saint-Etienne (ENSM.SE), 880 Avenue de Mimet, 13541 Gardanne, France
dutertre@emse.fr

[6] STMicroelectronics, Z.I. Rousset, 13106 Rousset CEDEX, France
mathieu.lisart@st.com

***Abstract*—Implementation attacks are a major threat to hardware cryptographic implementations. These attacks exploit the correlation existing between the computed data and variables such as computation time, consumed power, and electromagnetic (EM) emissions. Recently, the EM channel has been proven as an effective passive and active attack technique against secure implementations. In this paper, we review the recent results obtained on this subject, with a particular focus on EM as a fault injection tool.**

Keywords—Secure implementations; Side Channel Analysis; Fault Attacks; EM

I. INTRODUCTION

In the current society, a huge amount of information is sent and received in a digital form. In many domains, this information may be sensitive and may thus require to be protected against unauthorized access. Services such as confidentiality, integrity, and authentication can be provided by cryptographic protocols, which can be implemented in hardware when a high level of performance is required. Any weakness in the implementation of the cryptographic primitives would therefore be critical.

Attacks targeting directly the implementation are a very serious threat to the security of a system. Among all the attacks, those based on the observation of some physical quantity related to the data being computed (i.e., side channel) are perhaps the most dangerous, since they exploit the correlation between the values used in the secure computation and the electrical activity of the device. This channel may be the computation time, the power consumption, or, more recently, the electromagnetic (EM) emissions. Another class of attack, based on the active perturbation of the computation process by injection of errors, is more complex to put into practice, but even more dangerous in terms of efficiency of the attack. Several techniques can be used in order to perturb the computation: alterations in the operating environment, in the power supply, or in the clock signal; additionally, illumination by laser or EM waves can also provide a precise and effective technique of injecting errors into the circuit.

The EM emissions as an observation channel have been first considered in [1]. While the analysis of the power consumption can only reveal information at a global level, the EM channel allows focusing the observation on a specific local part of the circuit, namely the cryptographic coprocessor, without being masked by the contribution of the other blocks in the device. It is therefore much more precise and dangerous.

Electromagnetic waves can be used also as an active non-invasive medium of attack, although most research effort has been focused mainly on the generic problem of EM susceptibility. Moreover, the advancing fabrication process, aimed at increasing performance and reducing power

This work is partly supported by the French Ministry of Research, through the ANR project EMAISECI (act ANR-2010-SEGI-012-03). TIMA is Partner of the Labex PERSYVAL Lab (ANR-11-LABX-0025).

requirements, has as a collateral consequence that the circuits are also more vulnerable to external perturbations. Signals and components become more and more sensitive to transient perturbation at every technological step.

This paper presents the most recent results in the exploitation of the electromagnetic channel to mount attacks against a few building blocks of secure implementations, either by passive analysis or by active error injection. The paper is structured as follows: the next section describes the main technological issues related to the interaction between EM waves and cryptographic implementations. In Section III, we present the main results obtained for different targets and scenarios, in order to give a comprehensive picture of an EM attack. Section IV presents the more advanced issues, such as the complexity of specific experimental cases, and a deeper analysis of the interaction between the EM injection probe and the circuit logic. Existing and prospective countermeasures are discussed in Section IV.D. A quick overview of EM analysis is given In Section V. Finally, Section VI concludes the paper.

II. Devices and Technologies

Secure circuits like smartcard feature different functionalities among which the most important is the secure storage of secret data. To ensure the confidentiality and the integrity of secrets, cryptosystem must be able to encrypt/decrypt data by means of a secret key. In order to achieve this, cryptographic implementations are usually a combination of digital logic, used to implement the cryptographic algorithm, and analog logic, used to implement the clock tree (Embedded CLocK Generators, ECLKG) and random number generators (RNG), often used to generate temporary keys. The characteristics of analogue and digital blocks are radically different from a temporal point of view. This implies two different means of injecting EM perturbations in secure IC: one targeting critical analogue blocks such as ECLKG or RNG, and another one targeting the glue logic performing some digital cryptographic operations. We describe below the experimental setups and the results for both cases.

Analogue blocks can be attacked successfully by using powerful harmonic (continuous) waves. A stable sinusoidal signal must be generated at a given frequency, which is chosen either after analysis of the design or by experimentation, in order to maximize the effect of the injection. The goal of injecting such a harmonic wave is either to introduce a parasitic signal biasing the behavior of the block, or to inject some additional power directly and locally into the chip. Digital blocks on the other hand are clocked: to disrupt their behavior, EM pulse injection is preferable in order to inject faults in a specific clock cycle in a controllable way. It aims at injecting a sudden and sharp EM pulse into the IC so that intense transient currents, altering the behavior of logic cells, are produced.

The experimental setup for harmonic injection is depicted in Fig. 1. The system features several components: a motorized XY stage, modules for signal generation (data inputs and EM signal), the device itself, and an oscilloscope. The components are controlled by a PC, which is in charge of the configuration and the retrieval of the results. Fig. 2 shows instead the setup of the EM Pulse Injection platform. As shown, it features a high

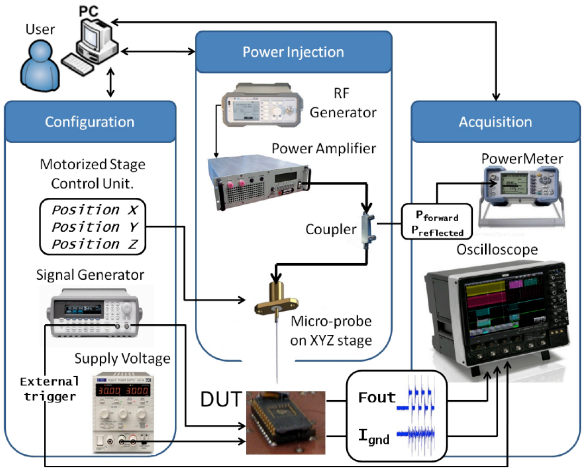

Fig. 1. Direct Power Injection Platform [2].

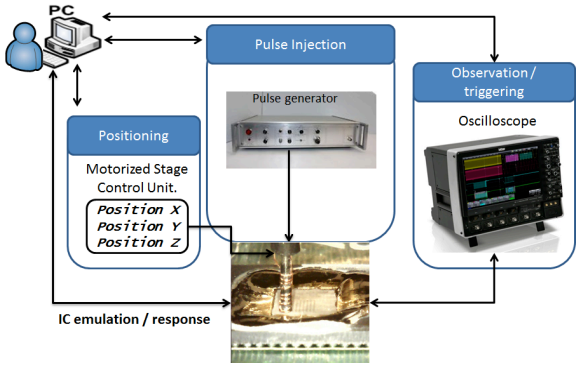

Fig. 2. EM pulse injection platform.

voltage pulse generator and a coil with a ferrite core as injection probe, rather than a thin tungsten rod as in Fig.1.

III. Main Results

A. Ring Oscillators

Ring oscillators are loops of combinational logic, usually chains of inverters, where the output of the chain is fed back at its input. Since there is no memory element within the loop, the state of such ring may continuously oscillate between low and high logic values, with characteristics which depend on the structure of the ring, the physical parameters of the specific implementation, and the environmental conditions. This construct is therefore often used as the basic building block for clock generators or Random Number Generators (RNG).

In [2], the authors have shown that with high frequency (1GHz) harmonic injection, it was possible to inject, locally into the chip, enough power into the power ground network to take control of an internal clock generator designed in 90nm. Additionally they have shown that the increase (up to 50%) of the frequency, Δf, of the internally generated clock signal was following the average supply voltage increase, ΔV, observed in presence of harmonic injection. This is illustrated in Fig. 3,

which shows the evolution of Δf and ΔV with respect to the power injected into the probe.

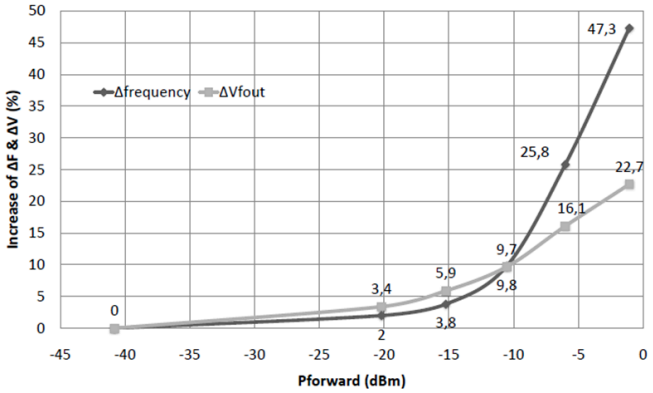

Fig. 3. Evolutions of Δf and ΔV with respect to to the power Pforward injected into the probe.

B. Random Number Generators

As it was presented in the last section, ring-oscillators are good candidates for TRNG design for both FPGA and ASIC implementations. Moreover, they can be also used for Physical Unclonable Function (PUF) design. However, one major constraint must be satisfied: all the ring oscillators must be completely independent. Still, it is possible to change the working conditions of the ring oscillators to make them dependent. A phenomenon of locking of the ring oscillators can then occur. This locking phenomenon was highlighted by Bochard et al. in 2010 by manipulating the supply voltage of the RO-based true random number generator (TRNG) [3]. Based on this preliminary study, we have used electromagnetic fault injection to change the behavior of ring oscillators embedded in FPGA [4]. We have also used the electromagnetic channel to collect information such as the oscillator frequency and the physical location of the oscillators inside the chip [5]. Similar results were obtained in [6] when the target was specifically RO-PUF. These works clearly challenge the use of ring oscillators for TRNG and PUF design. The security requirements for TRNG and PUF designs are: (1) that ring oscillators have to be completely independent; and (2) that the frequency of the ring oscillator has to be hidden. Because of electromagnetic attacks, these requirements are no longer guaranteed.

To illustrate that we are able to manipulate the RO-TRNG behavior with electromagnetic harmonic injection, Fig. 4 shows the TRNG output bitstream produced at several levels of

Fig. 4. Fault occurrence rate versus pulse amplitude [4].

electromagnetic injected power during the experiments (targeting FPGA implementation [4]). Each sample is composed of 120 successive 32-bit frames (black and white squares corresponding to ones and zeros, respectively). Note that under normal conditions (Figure 2.a), the RO-TRNG bitstream passed NIST statistical tests applied on 1000 sequences of 1 Mbit. At higher injected power, the output becomes clearly biased.

C. Cryptographic Co-Processors

In [7], the authors attacked an AES implemented on a Xilinx Spartan 3. The architecture is quite straightforward: a communication and control module, an on-the-fly key expansion module, and an iterative encryption module were implemented on the programmable chip.

The whole surface of the package was exposed to localized EMPs with a displacement step equal to the probe diameter. This gave a total of 30x30 injection locations, shot 1000 times each during the last round of the encryption. Results are shown in Fig. 5, where the injection cartography (on the right) is associated to the floorplan of the design (on the left). It can be seen that the effects of EM pulses are clearly local, and that there is a good correlation between the most sensitive regions and the placement of the AES logic (both encryption round and key scheduler). Additionally, there is also a clear symmetry which is not coming from the implemented design, but rather from the geometric layout of the programmable chip. This will be further discussed in Section IV.B

D. General Purpose CPUs

In [8], the authors performed an attack on an up-to-date 32-bit microcontroller based on the ARM Cortex-M3 processor. Their attack targeted the round counter of a software AES implementation. They used a pulsed electromagnetic fault injection technique to skip a chosen assembly instruction and add an extra encryption round. Then, they proposed a cryptanalysis to recover the encryption keys by using the faulty outputs.

A more in-depth analysis of the effect of electromagnetic pulses has been provided in [9]. In this article, the authors showed the influence of some electromagnetic injection experimental parameters by performing attacks on some isolated assembly instructions. More precisely, they studied the influence of the injection antenna's position over the circuit, the injection time, and the pulse's electrical characteristics. On the selected target, they managed to force some data transfers from the memory to `0xFFFFFFFF` by targeting a single `ldr` instruction (that loads a piece of data from the memory into a register). By performing attacks on a sequence of `nop` instructions, they also highlighted the fact that some binary opcodes could be corrupted and some instructions could be

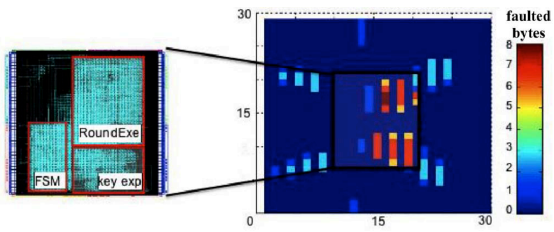

Fig. 5. Floorplan of the AES implementation and associated fault injection cartography [7].

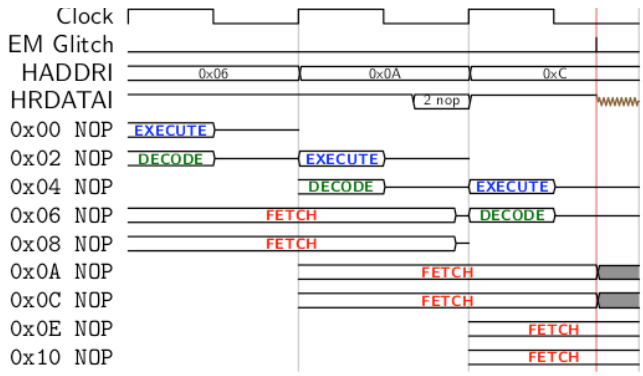

Fig. 6. Bus transfers on the Cortex-M3 instruction bus with an electromagnetic glitch fault injection [9].

replaced by others. In their experiments, they managed to execute a `str` instruction (that stores a register into the memory) instead of a `nop` by using a fault injection.

According to their analysis, the bus transfers from the Flash memory (both for instructions and data) can be corrupted by an electromagnetic pulsed fault injection. The Flash memory has a long response time for bus transfers. Thus, on an AMBA AHB bus, the value to transfer is written on the bus at the end of a clock cycle. Bus transfers and pipeline stages during the execution of a `nop` sled are shown on Fig. 6. Since instruction fetches are 32-bit wide, two 16-bit `nop` are loaded at each *fetch* pipeline stage. This figure shows that the two fetched instructions are written on the bus at the end of a clock cycle and thus are corrupted by an electromagnetic glitch. To sum up, the fault injection technique used in this paper induces timing constraint violation faults [7]. Thus, it seems that because of their low slack such bus transfers are the first to be hit.

IV. Advanced Modeling

A. Harmonic EM injections targeting RO-TRNG

Besides the direct effect on the ring oscillators involved in the RO-TRNG structure (i.e., the phenomenon of RO locking depicted in [5]), other effects are observed during RO-TRNG attacks by harmonic EM injection. These effects conduct to the two following faults on the D flip-flop used for RO signal sampling:

- Flip-flops tend to erroneously sample on some falling edges of the clock signal.
- Some values sampled on the rising edge are not correct (meaning that either the flip-flop did not sample, or that the value sampled was corrupted, or that the sampling time moved slightly, due to some added jitter on the clock signal).

Note that compared to the first fault, the second fault appears to occur only rarely.

To study the fault model on the D flip-flop we have used two models. The first one, depicted in Fig. 7, models the EM injection as a sinusoidal generator connected to the clock tree. The second one, depicted in Fig. 8, models the EM injection as two sinusoidal generators connected to the two power lines of the circuit (ground and Vdd).

The two models provide the same faulty behavior that is observed during the experimental attacks on FPGA [3]. So, there are both "electrically" correct. Nevertheless, FPGA devices usually consist of several complex circuits featuring:

- A power supply mesh with lots of loops.
- A clock tree that is mainly composed of long lines (rods) which cross the whole circuit and provide constant clock skew at every destination point of the device.

The power supply mesh tends to be disturbed by magnetic fields, while the clock tree is mostly disturbed by electric fields (see [10][11]). For these reasons, the first model is best for describing attacks using electric fields, while the second model is best for describing attacks using magnetic fields. Since during experimental attacks we only used electric probes, the first fault model modeling disturbances in the clock tree (clock signal) is physically correct.

B. Pulsed EM Injections

The experiments conducted in [7] highlighted a strong resemblance to errors originated by delay faults. If the injected power is increased gradually on the same spot, the probability of injecting an error increases (see Fig. 9). Moreover, faults

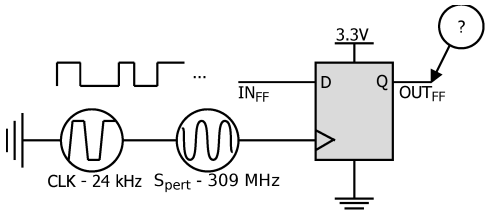

Fig. 7. First electrical fault model of EM harmonic injection targeting the D flip-flop of a RO-TRNG.

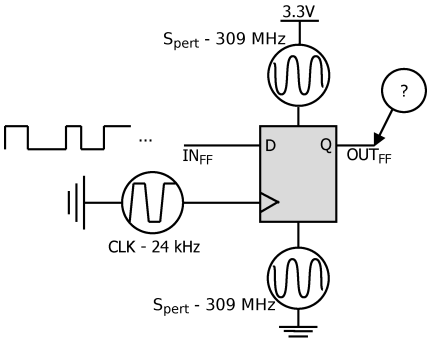

Fig. 8. Second electrical fault model of EM harmonic injection targeting the D flip-flop of a RO-TRNG.

injected by applying precise clock glitches on the same design led to very similar error patterns. This assumption was further supported by the experiments run on a design protected with a configurable delay guard, where the propagation latency could be chosen at runtime. The patterns and mechanisms of alarm triggering were consistent with the initial hypothesis of delay faults.

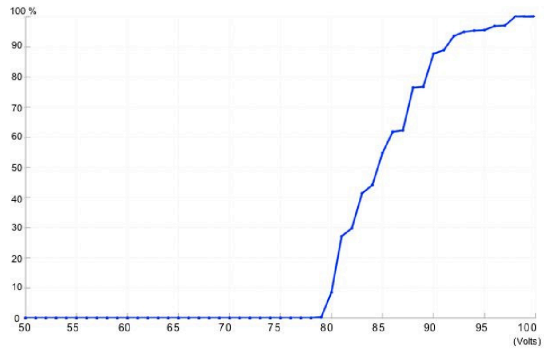

Fig. 9. Fault occurrence rate versus pulse amplitude [7].

This behavior can be explained by the fact that the EM pulse probably interacts with the power-ground network of the circuit: an additional amount of energy is thus delivered to the network, which alters the differential voltage supply (i.e., it lowers the difference between the supply voltage and the ground, either by lowering V_{dd} or by increasing the ground itself). Where the logic is under the influence of the EM pulsed injection, combinational ports are locally fed by a slightly lower tension, which makes them react more slowly to the propagation of the signal transitions. If the slowdown is larger than the available slack in the targeted paths, data cannot reach the input of the flip flops within the delay, the timing constraints are violated and a transient error is thus captured.

As stated above, delay faults can be obtained also through perturbations to the clock (a shorter period for one or a few cycles) or to the supply (lower than the nominal value). These perturbations make the clock period shorter than the critical path of the circuit. Unlike these techniques, however, EM pulsed injections have the undeniable advantage of acting locally: this means that specific locations of the circuit can be targeted, conformingly to the experimental parameters: technology of the circuit, size and shape of the used probe, and delivered power.

C. *EM Power Coupling*

As anticipated in the previous section, understanding and predict the consequences of an EM pulsed injection onto a secure circuit is a critical challenge. In order to achieve this, three main issues need to be solved: a model of the injection probe; a model of the power coupling between the EM wave and the circuit layers; and finally, a model of the circuit operating under altered conditions.

A detailed model of the probe allows knowing the shape and the intensity of the EM field created during the injection: with this information, the designer is able to know precisely the energy delivered to the circuit in every sub-region. The creation of such model is partly theoretical and partly experimental, and several works already exist.

When the power delivered by the probe to the surface of the circuit is known, it is possible to calculate the amount of energy that is reflected or absorbed by each layer of the circuit [12]. To achieve this, the layout of the circuit and the parameters of the fabrication process must be known. The end result is that the amount of energy delivered to the target region can be estimated quite precisely.

The amount of energy delivered to a specific region of the circuit can hence be used to simulate the behavior of the design. Before the fabrication of the first prototypes, the design must undergo a series of validation tests (sign-off analyses), being the IR-drop analysis one of them. This process ensures that the fluctuations of power supply, due to the dynamic load, do not affect the functionality of the circuit. Dedicated tools exist, which allow simulating the circuit under the hypothetical condition of an additional current generator (*what-if* analyses): a generator can thus be placed, dimensioned in function of the energy delivered by the electromagnetic pulse, and the circuit simulated under these faulty conditions in order to predict its behavior during an EM fault attack.

D. *Countermeasures against Electromagnetic Injection*

It has been shown in the previous sections how electromagnetic pulsed injections can cause local delay faults. On this basis, the most suited countermeasure can be chosen. In general, error detection is based on some form of redundancy, either based on resources, time, or information.

Hardware redundancy uses two or more instances of a functional block to compare the results and detect any differences. If the blocks are far enough, then an EM pulse will hardly affect both instances in the same way; however, this is difficult to prove and it may depend on specific properties of the design. Moreover, the protection might fail if the attacker is able to shoot a strong enough pulse. Temporal redundancy is based on the repetition of the competition on the same hardware. Even if EM faults are transient, repeatability is quite high and this approach should be therefore avoided. Information redundancy uses error detecting codes to identify a perturbation in the computation process: their effectiveness depends, however, on the level of redundancy and they are more oriented to natural faults. They may thus become quite expensive or ineffective in the context of fault attacks.

A more targeted countermeasure has been presented in [7], consisting in a generic solution detecting timing violations. It is based on a chain of multiplexers, whose length can be configured at runtime through proper setting of the control signals. Since the propagation delay of the multiplexer chain depends also on the supply voltage, as the rest of the circuit logic, it will be equally affected by the EM injection. If the pulse is strong enough to violate the timing constraint of the chain, then an alarm will be triggered. Obviously, the critical path of the detector chain must be properly set between the longest critical path of the circuit and the clock period, in order to avoid non detection and false positives. The placement of several detectors has been evaluated in [13]: up to 5 detectors were added to the implementation, with a negligible overhead. On the other hand, the number or the placement of the detectors was not optimal, since the authors were still able to bypass the countermeasure with a success rate of about 10%. Given the low cost of the solution, however, it is possible to increase the number of detectors in order to obtain a better protection.

analysis [14].

	Power			EM		
Design	Key bytes found	Mean Guessing Entropy	# traces ($\times 10^3$)	Key bytes found	Mean Guessing Entropy	# traces ($\times 10^3$)
Unprotected	15	1	205	16	1	155
Solution 1	4	54	275	8	52	275
Solution 2	5	34	287	9	17	287
Solution 3	7	19	250	12	9	250
All solutions at same time	0	136	283	0	94	283

V. ELECTROMAGNETIC ANALYSIS

So far, we did not consider the electromagnetic channel as a passive source of information. Just as power consumption, however, EM emissions can be recorded and analyzed through statistical analysis (differential, correlation, or mutual information analysis, for instance) in order to discover the secret information. Moreover, the information delivered by the EM channel is much richer, since it does not give a limited global summary of the circuit, but on the other hand carries also a significant content of spatial and frequency information. Table I [14] shows the results for both EM and power analysis on an AES design equipped with a few countermeasures against side channel analysis. The results are shown in terms of number of key bytes revealed, number of traces required to obtain those results, and the mean Guessing Entropy, that is the average ranking of the correct key among all possible hypotheses. It can be seen that the EM channel is much more effective when it comes to side channel attacks.

The countermeasures that can be used to counteract EM analysis are usually the same proposed against power analysis: data masking, dual rail logic and additional noise can all contribute to decrease the correlation between the side channel leakage and the secret key. It is important to observe, however, that the spatial connotation of EM emissions makes these solutions less effective; additionally, it could also be exploited to mount higher order attacks on different locations of the circuit, aiming at suppressing the contribution of the random masks.

An attempt at designing a countermeasure addressing the spatial richness of the EM channel has been proposed in [14] and [15]: in these works, computations are allocated on different resources each time, thus decreasing the correlation between the traces and the key. Their cost, however, is not negligible, and the protection is often not sufficient, demanding for additional countermeasures as well.

VI. CONCLUSION

Physical attacks can be a very serious threat to secure implementations. Electromagnetic analysis and fault injection, in particular, are very effective means of revealing the secret information. In this paper, we have summarized the most recent results in several scenarios, from analog blocks to general purpose CPUs. In all situations, the EM channel has proven to be a rich, powerful, and promising technique to attack secure circuits. The results have clearly shown that EM attacks need to be considered early in the design phase and that suitable tools and methodologies must be adopted.

REFERENCES

[1] J.-J. Quisquater and D. Samyde. *Electromagnetic analysis (EMA) : Measures and counter-measures for smart cards*. In E-smart, pages 200-210, 2001.

[2] F. Poucheret, K. Tobich, M. Lisart, L. Chusseau, B. Robisson, P. Maurine: *Local and Direct EM Injection of Power Into CMOS Integrated Circuits.* FDTC 2011: 100-104.

[3] N. Bochard, F. Bernard, V. Fischer, B. Valtchanov: *True-Randomness and Pseudo-Randomness in Ring Oscillator-Based True Random Number Generators*. Int. Jour. of Reconfigurable Computing, Hindawi, Vol. 2010, ID 879281, 13 pages, 2010.

[4] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, P. Maurine: *Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator*. COSADE 2012: 151-166.

[5] P. Bayon, L. Bossuet, A. Aubert, V. Fischer: *EM leakage analysis on True Random Number Generator: Frequency and localization retrieval method*, in Proc. of Asia-Pacific Int. Symp. And Exh. On Electromagnetic Compatibility (APEMC), 2013.

[6] D. Merli, D. Schuster, G. Sigl: *Semi-invasive EM attack on FPGA RO PUFs and Countermeasures* In Proc. of the Workshop on Embedded Systems Security (WESS). ACM, New York, NY, USA, 2011, Article 2, 9 pages.

[7] A. Dehbaoui, J.-M. Dutertre, B. Robisson, A. Tria: *Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES*. FDTC 2012: 7-15.

[8] A. Dehbaoui, A.-P. Mirbaha, N. Moro, J.-M. Dutertre, A. Tria: *Electromagnetic Glitch on the AES Round Counter*. In COSADE 2013: 17-31

[9] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, E. Encrenaz: *Electromagnetic Fault Injection : Towards a Fault Model on a 32-bit Microcontroller*. In FDTC 2013: 77-88

[10] S. Ben Dhia, M. Ramdani and E. Sicard: Case Studies EMC Test-chips, low-emission microcontrollers, Electromagnetic Compatibility of Integrated circuits: Technique for Low Emission and Susceptibility 2006, Springer, Chapter 6, 311-314.

[11] X. Dong, S. Deng, T. Hubing and D. Beetner: *Analysis of chip-level EMI using near-_eld magnetic scanning*. International Symposium on Electromagnetic Compatibility, EMC 2004, IEEE, pp.174-177.

[12] D. Alberto, P. Maistri, R. Leveugle: *Electromagnetic Attacks on Embedded Devices: a Model of Probe-circuit Power Coupling*. DTIS 2014: to appear.

[13] L. Zussa, A. Dehbaoui, K. Tobich, J.M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clédiere, and A. Tria: Efficiency of a Glitch Detector against Electromagnetic Fault Injection. Design Automation and Test in Europe (DATE), 2014.

[14] P. Maistri, S. Tiran, P. Maurine, I. Koren, R. Leveugle: *Counter-measures against EM analysis for a secured FPGA-based AES implementation*. ReConFig 2013: 1-6.

[15] F. Poucheret, L. Barthe, P. Benoit, L. Torres, P. Maurine, M. Robert: *Spatial EM jamming: A countermeasure against EM Analysis?* In VLSI-SoC 2010: 105-110.